REMARKS

Prior to entry of this paper, Claims 1-20 were pending. Claim 1-20 were rejected. In this paper, Claim 12 is amended; no claims are canceled, or added. Claims 1-20 are currently pending. No new matter is added by way of this amendment. For at least the following reasons, Applicants respectfully submit that each of the presently pending claims is in condition for allowance.

Examiner Interview:

The Applicants wish to thank the Examiner and his supervisor for taking the time to discuss the pending applications and the cited prior art references with the Applicants' representative. The discussion was directed to how the Applicants believe Benaloh fails to address each of the limitations of at least claim 18. While no consensus was reached, it was stated that the discussion may have provided the Examiner with a different understanding of the cited reference. It was also noted that Claim 18 may have been improperly rejected, as the Examiner may have included elements in the examined claim that were deleted in a prior office action response.

Claim Rejections

Claims 1-3, 5-8, 10, and 11 are rejected under 35 USC 102(e) as being anticipated by Benaloh et al., U.S. Patent No. 7,065,216 (hereinafter Benaloh). Claims 4, 9, 12-20 are rejected under 35 USC 103(a) as being unpatentable over Benaloh in view of Cooper et al., US PGPUB No. 20010051996 (hereinafter Cooper). Applicants respectfully traverse these rejections.

For example, nowhere does the cited prior art references either alone or in combination teach or suggest receiving a first wrapper of content sent to a second market participant that is associated with the network device (configured to perform the actions), decrypting the content, generating at least one of a fingerprint or a watermark that uniquely identifies the second market participant, and marking the decrypted content by embedding the fingerprint or watermark into the decrypted content.

Benaloh fails to teach such limitations, as was discussed during the Examiner's interview. Instead, Benaloh appears to describe each of individual partitions of content being separately and uniquely marked, as by any suitable fingerprinting or watermarking technique. See Benaloh's Figure 9, and Col. 9 lines 2-19. Individual different keys are then associated with each of the uniquely marked partitions. These keys are utilized to encrypt the partitions to provide respective partitions. See Benaloh's Figure 9, and Col. 9 lines 45-60. Next, individual unique key collections are defined which, in any one key collection, there appears one and only one key for one partition or clip in each partition set. See Benaloh's Figure 9, and Col. 9 lines 61-67. Each unique key collection is then associated with a corresponding content player and encrypted with that content player's public device key…only the content player with the corresponding private device key can decrypt the encrypted key collection to access the encrypted content. See Benaloh, Col. 10 lines 4-19. Thus, it can be seen that Benaloh's watermark or fingerprints alone do not uniquely identify the second market participant (that is the market participant that received the content and decrypted the content). Instead, it is the unique public/private key pair that uniquely identifies for Benaloh the content recipient, and then only through that relationship the marked content. Thus, for at least this reason, Benaloh fails to teach or even suggest generating at least one of a fingerprint or a watermark that uniquely identifies the second market participant, and marking the decrypted content by embedding the fingerprint or watermark into the decrypted content as required by at least Claim 18.

Moreover, unlike at least claim 18, the watermarking of the content is not performed in Benaloh by the recipient of the content (the second market participant), but instead appears to be watermarked or fingerprinted by an entity that subsequently delivers the content to each player. See Benaloh's Figures 2 and 12 (block 1216). Thus, Benaloh does not teach or even suggest that the watermarking is performed by the same entity that first decrypts the content, as required by at least Claim 18, as noted by receiving a first wrapper of content including encrypted content (by the network device associated with the second market participant), decrypting the encrypted content, and marking the decrypted content by embedding the fingerprint or watermark into the decrypted content (that uniquely identifies the second market participant).

Moreover, because Benaloh relies upon the public/private keys to uniquely identify the recipient of the marked content, sending of the watermarked content to yet another recipient by the first recipient would then likely break the relationship established by Benaloh's first content sender between the collection of watermarked partitions and public/private key pair. Thus, Benaloh further fails to teach or suggest being able to transmit the second wrapper to the third market participant, as recited in at least Claim 18. For at least these reasons, at least Claim 18 is allowable.

Independent Claim 1 includes similar, albeit different, limitations as Claim 18. For example, Claim 1 also recites receiving the content, decrypting the content, determining a self-identifier that uniquely identifies an entity decrypting the content and modifying the decrypted content by embedding at least one or a fingerprint or a watermark...wherein the fingerprint or watermark is generated, in part, from the self-identifier. Clearly, Benaloh does not teach or suggest watermarking decrypted content as recited in at least Claim 1. Similarly, Claims 12 and 20 includes similar, albeit different, limitations as Claims 1 and 18. Cooper fails to teach such limitations and instead teaching watermarking the content and then transferring (downloading) that content to the user. See Cooper Figure 3. Therefore, Applicants submit that the cited prior art references either alone or in combination, fail to anticipate or render obvious at least claims 1, 12, 18, and 20. Thus, for at least the same reasons as Claim 18, at least Claims 1, 12, and 20 are also allowable.

Moreover, Claim 7, which depends from Claim 1 further recites providing the wrapped modified content to a downstream market recipient, decrypting the received content by the downstream market recipient, and further modifying the decrypted modified content by embedding another fingerprint or watermark into the modified content...that uniquely identifies the downstream market recipient that decrypts the modified content. As is clear, the combination of Claims 1 and 7 result in multiple decrypting and multiple watermarking of the content, each watermarking being performed by that which has decrypted the content and where the watermark uniquely identifies who decrypted the content. Such multiple entities doing such actions are clearly not taught nor suggested by Benaloh. Thus, for at least these reasons, Claim 7 is also allowable.

Moreover, claims 2-11, 13-17, and 19 depend from claims 1, 12, and 18, respectively. Therefore, they are also allowable for at least the same reasons as claims 1, 12, 18, and 20. The Applicants thus respectfully request that these claims also be allowed to issue.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-20) is in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicants reserve the right to raise these arguments in the future.

Dated: January 17, 2008   Respectfully submitted,

By _Jamie L. Wiegand_

Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(206) 262-8915
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant